CLAIMS

What is Claimed is:

1. A method of secure communication of an electronic document from a sender to a recipient, verification of sending of the electronic document by the sender and verification of the receipt of the electronic document by a recipient, in association with at least one third party, comprising the steps of:

the sender generating a substantially unique and substantially undecryptable first digital string based upon said electronic document and communicating said first digital string to said at least one third party;

the sender encrypting first and second unencrypted portions of said electronic document with respective first and second encryption algorithms thereby generating respective first and second encrypted portions and communicating said first and second encrypted portions to said at least one third party;

said at least one third party notifying said recipient of said first and second encrypted portions and, in response to a request from said recipient, communicating said first and second encrypted portions to said recipient;

said recipient using a first decryption algorithm thereby generating said first unencrypted portion;

said at least one third party, in response to a request from said recipient, communicating to said recipient said first digital string and a decryption key for decrypting output of said second encryption algorithm; and

said recipient using said decryption key to generate said second unencrypted portion, said recipient further generating a substantially unique and substantially undecryptable second digital string based upon said first and second unencrypted portions of said electronic document and comparing said first digital string to said second digital string.

2. The method of Claim 1 wherein said step of communicating said first digital string to said at least one third party further includes the step of communicating a

first number identifying the sender and a second number identifying the recipient.

3. The method of Claim 2 wherein said step of communicating said first digital string and said step of communicating a first number and a second number further includes the step of the sender encrypting said first digital string, said first number and said second number by a third encryption algorithm.

4. The method of Claim 3 wherein said third encryption algorithm is an asymmetric encryption algorithm employing an asymmetric encryption key and an asymmetric decryption key associated with said at least one third party.

5. The method of Claim 1 wherein said second encrypted portion is generated by encrypting said second unencrypted

portion by the second encryption algorithm and said first encryption algorithm and wherein said step of said recipient using a first decryption algorithm further includes using the first decryption algorithm on said second encrypted portion.

6. The method of Claim 1 further including the step of the recipient communicating a message ultimately destined for the sender indicating results of the step of comparing said first digital string to said second digital string.

7. A method for a recipient to receive and decrypt an encrypted electronic message and verify receipt and decryption thereof, comprising the steps of:

requesting communication of said encrypted electronic message and a message identifying number in response to notification of said encrypted electronic message, said electronic message including a first encrypted document portion encrypted by at least a first encryption algorithm and a second encrypted document portion encrypted by at least a second encryption algorithm, said first encryption algorithm being different from said second encryption algorithm;

decrypting said first encrypted document portion to obtain a first decrypted document portion;

transmitting a request for a decryption key for said second encryption algorithm, said request including said message identifying number;

receiving said decryption key in response to said transmitting step, and further receiving a substantially unique and substantially undecryptable first digital string based upon said encrypted electronic message prior to encryption;

decrypting said second encrypted document portion using said decryption key to obtain a second decrypted document portion;

generating a substantially unique and substantially undecryptable second digital string based upon said first and second decrypted document portions, said first and second decrypted document portions intended to comprise decryption of said encrypted electronic message;

comparing said first digital string to said second digital string; and

transmitting a message indicating a result of said comparing step.

8. The method of Claim 7 wherein said requesting step is performed in response to manual input by the recipient.

9. The method of Claim 7 wherein said second portion of the encrypted message is further encrypted by the first encryption algorithm using said first encryption key, and wherein said step of decrypting said first encrypted document portion further includes said portion of the encrypted message thereby removing one level of encryption on said second portion of the encrypted message.

10. A method for establishing an evidentiary trail substantially establishing that a recipient has received an encrypted message and decrypted the encrypted message, comprising the steps of:

recording that the recipient has been notified of the encrypted message;

recording that the recipient has requested the encrypted message;

recording that the encrypted message has been communicated to the recipient, said encrypted message including a first encrypted portion and a second encrypted portion, wherein the first encrypted portion has been encrypted by at least a first encryption algorithm and the second encrypted portion has been encrypted by at least a second encryption algorithm, wherein the recipient uses a first decryption key to decrypt the first encrypted portion, but must receive a second decryption key to decrypt the second encrypted portion;

recording that the recipient has requested said second decryption key associated with the encrypted message;

recording that the recipient has received said second decryption key associated with the encrypted message and has further received a substantially unique and substantially undecryptable first digital string based upon said encrypted message prior to encryption; and

recording that the recipient has transmitted a message verifying that said decryption key has been received, that said second encrypted portion has been decrypted and that the recipient generated a substantially unique and substantially undecryptable second digital string based on decryption of said encrypted message which matches said substantially unique and substantially undecryptable first digital string.

11. The method of Claim 10 wherein said step of recording that the encrypted message and a message identifying number has been communicated to the recipient further includes the step of recording that said first encryption key has been communicated to the recipient.

12. The method of Claim 11 wherein said step of recording that the encrypted message has been communicated to the recipient further includes the step of recording that a message identifying number has been communicated to the recipient.

13. The method of Claim 12 wherein said step of recording that the recipient has requested said second decryption key further includes the step of recording that the recipient has transmitted said message identifying number.

14. The method of Claim 10 wherein said second portion of the encrypted message is further encrypted by the first encryption algorithm using said first encryption key.

15. A method of establishing an evidentiary trail substantially establishing that a sender has transmitted an

encrypted message, the evidentiary trail substantially establishing contents of the encrypted message prior to encryption while substantially maintaining confidentiality of the unencrypted contents of the encrypted message, comprising the steps of:

recording that the sender has communicated a substantially unique and substantially undecryptable digital string based upon said encrypted message prior to encryption and a number identifying an intended recipient;

recording that the sender has received a first encryption key, a second encryption key, a third encryption key, a document identification number substantially unique to the encrypted message, an encrypted version of said identification number, said digital string; and

recording that the sender has communicated said encrypted message comprising a first portion of the encrypted message encrypted by at least a first encryption algorithm using said first encryption key and a second portion of the encrypted message encrypted by at least a second encryption algorithm using said second encryption key; and has further communicated said number identifying the intended recipient, said document identification number, and said third encryption key.

16. The method of Claim 16 wherein said step of recording that the sender has received a first encryption key further includes the step of recording that the sender has received an identification number associated with the encrypted message, and a third encryption key associated with the recipient.

17. The method of Claim 17 wherein said step of recording that the sender has communicated said encrypted message further includes the step of recording that the sender has communicated a title associated with said encrypted message.

18. The method of Claim 18 further including the step of recording that the sender has received a message indicating status of reception and decryption of said encrypted message by the intended recipient.

19. The method of Claim 15 wherein said second portion of the encrypted message is further encrypted by said first encryption algorithm using said first encryption. key.